Statewide Information Security and Policies

Enterprise Security

The Enterprise Security and Risk Management Office (ESRMO) exists to support a comprehensive statewide information security and risk management program that includes several areas of focus:

- Information Security Awareness
- Threat and Vulnerability Management
- Cyber Incident Management
- Risk and Business Continuity Management

Agency Security Liaisons

- Each agency is required by law to have a security liaison who acts as a primary point of contact to the State Chief Information Officer.
- Security liaisons coordinate requests for security information, ensure cyber security incidents are reported, and provide input to Statewide Information Security Manual.
- The agency security liaison for ITS is Charles “Chip” Moore.

Statewide Information Security Manual?

- The Statewide Information Security Manual is the foundation for information technology security in North Carolina.
- The Manual contains the common policies and information security standards that all executive branch agencies much comply and is based on ISO 27002 and references several NIST standards.
- The security standards within the Manual have been extensively reviewed by representatives of each executive branch agency and are continuously reviewed as needed.

Why Statewide Policies?

- G.S. §147-33.110 directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security.

- The Statewide Information Security Manual is the baseline for information security for all agencies. While executive branch agencies are required to follow the statewide information security standards, each agency should have additional policies specific to its business and practice.

- While not mandated, local governments, LEAs, community colleges, constituent institutions of the University of North Carolina and other public agencies are encouraged to follow it.

Where is the Statewide Manual?

- The Statewide Information Security Manual is located on the State CIO’s website at the following address:

https://www.scio.nc.gov/mission/itPoliciesStandards.aspx

- There are 15 chapters in the manual. Each standard has a number that corresponds to the chapter and section of that chapter.

Policy Review

- There is a review process for the Statewide Information Security Manual. The ESRMO solicits recommendations from the agencies and creates a plan for updating the manual.

- The ESRMO reviews suggestions from the agencies, as well as researches various state and federal standards and industry best practices and then recommends to the State CIO changes to policy manual. The updated manual is published on the State CIO’s website.

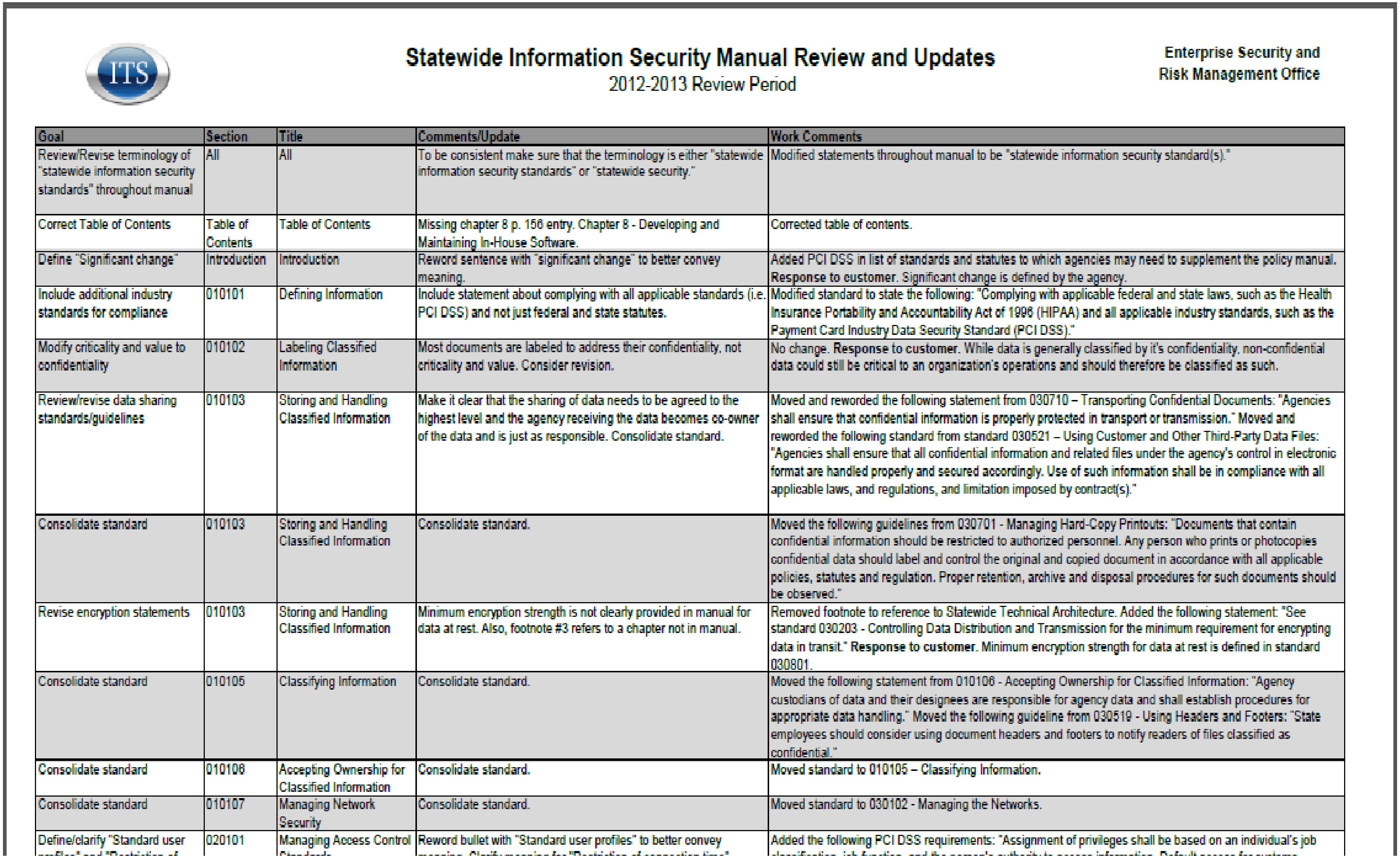
- Questions, comments and suggestions are welcome at any time. Recommendations for change outside of the review period will be saved for the next review period.

New Updates

The 2013 version of the policy manual included the following updates:

- Reduced/Moved content
- Clarified some requirements
- Added some new requirements
- Included PCI DSS requirements

New Updates



Statewide Information Security Manual Review and Updates

2012-2013 Review Period

Enterprise Security and Risk Management Office

Goal	Section	Title	Comments/Update	Work Comments
Review/Revise terminology of "statewide information security standards" throughout manual	All	All	To be consistent make sure that the terminology is either "statewide information security standards" or "statewide security."	Modified statements throughout manual to be "statewide information security standard(s)."
Correct Table of Contents	Table of Contents	Table of Contents	Missing chapter 8 p. 156 entry. Chapter 8 - Developing and Maintaining In-House Software.	Corrected table of contents.
Define "Significant change"	Introduction	Introduction	Reword sentence with "significant change" to better convey meaning.	Added PCI DSS in list of standards and statutes to which agencies may need to supplement the policy manual. **Response to customer**. Significant change is defined by the agency.
Include additional industry standards for compliance	010101	Defining Information	Include statement about complying with all applicable standards (i.e. PCI DSS) and not just federal and state statutes.	Modified standard to state the following: "Complying with applicable federal and state laws, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all applicable industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS)."
Modify criticality and value to confidentiality	010102	Labeling Classified Information	Most documents are labeled to address their confidentiality, not criticality and value. Consider revision.	No change. **Response to customer**. While data is generally classified by it's confidentiality, non-confidential data could still be critical to an organization's operations and should therefore be classified as such.
Review/revise data sharing standards/guidelines	010103	Storing and Handling Classified Information	Make it clear that the sharing of data needs to be agreed to the highest level and the agency receiving the data becomes co-owner of the data and is just as responsible. Consolidate standard.	Moved and reworded the following statement from 030710 – Transporting Confidential Documents: "Agencies shall ensure that confidential information is properly protected in transport or transmission." Moved and reworded the following standard from standard 030521 – Using Customer and Other Third-Party Data Files: "Agencies shall ensure that all confidential information and related files under the agency's control in electronic format are handled properly and secured accordingly. Use of such information shall be in compliance with all applicable laws, and regulations, and limitation imposed by contract(s)."
Consolidate standard	010103	Storing and Handling Classified Information	Consolidate standard.	Moved the following guidelines from 030701 - Managing Hard-Copy Printouts: "Documents that contain confidential information should be restricted to authorized personnel. Any person who prints or photocopies confidential data should label and control the original and copied document in accordance with all applicable policies, statutes and regulation. Proper retention, archive and disposal procedures for such documents should be observed."
Revise encryption statements	010103	Storing and Handling Classified Information	Minimum encryption strength is not clearly provided in manual for data at rest. Also, footnote #3 refers to a chapter not in manual.	Removed footnote to reference to Statewide Technical Architecture. Added the following statement: "See standard 030203 - Controlling Data Distribution and Transmission for the minimum requirement for encrypting data in transit." **Response to customer**. Minimum encryption strength for data at rest is defined in standard 030801.
Consolidate standard	010105	Classifying Information	Consolidate standard.	Moved the following statement from 010106 - Accepting Ownership for Classified Information: "Agency custodians of data and their designees are responsible for agency data and shall establish procedures for appropriate data handling." Moved the following guideline from 030519 - Using Headers and Footers: "State employees should consider using document headers and footers to notify readers of files classified as confidential."
Consolidate standard	010106	Accepting Ownership for Classified Information	Consolidate standard.	Moved standard to 010105 – Classifying Information.
Consolidate standard	010107	Managing Network Security	Consolidate standard.	Moved standard to 030102 - Managing the Networks.
Define/clarify "Standard user	020101	Managing Access Control	Reword bullet with "Standard user profiles" to better convey	Added the following PCI DSS requirements: "Assignment of privileges shall be based on an individual's job

Deviation Process

- A deviation is a situation in which an agency information technology resource is out of compliance with the Statewide Information Security Manual. A deviation may put information systems and/or data at risk of damage, loss or exposure.
- The deviation reporting process is intended to report deviations. *It is not designed to request a deviation!* There must be a compelling business need to allow a deviation.
- Every deviation report requires detailed information about the deviation and the signature of the application owner or IT Manager AND the agency security liaison before submission.
- The ESRMO processes all deviation reports. The State CIO ultimately approves or denies deviation reports.

Questions?